DIALOG(R)File 352:Derwent WPI

013690285 **Image available**
WPI Acc No: 2001-174509/200118
XRPX Acc No: N01-126391
IC card identification with fingerprints involves operating card reader interface circuit to exchange card information in memory to host computer, when IC card owner is legitimate by analyzing his fingerprints
Patent Assignee: SHEN M X (SHEN-I)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2001005945	A	20010112	JP 99229629	A	19990816	200118	B

Priority Applications (No Type Date): TW 99U209054 U 19990603
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2001005945	A		7	G06K-019/10	

Abstract (Basic): JP 2001005945 A

NOVELTY - The fingerprint of the IC card owner is scanned by sensor (12) and then the scanned data is compared with the data in memory (11). When the IC card owner is judged to be a legitimate user, based on the comparison result, the microprocessor (14) operates the card reader interface circuit (13) in order to exchange card information via card reader (2) to host computer (3) from memory (11).

USE - In cash transaction security when using credit card, money card etc., for identification of IC card using fingerprints of IC card.

ADVANTAGE - The risk accompanying when the IC card is lost or forgot, is reduced as the IC cards are used only after confirming whether the user is a legitimate user.

DESCRIPTION OF DRAWING(S) - The figure shows block diagram of IC card identifier apparatus.

Card reader (2)
Host computer (3)
Memory (11)
Sensor (12)
Card reader interface circuit (13)
Microprocessor (14)
pp; 7 DwgNo 1/5

Title Terms: IC; CARD; IDENTIFY; FINGERPRINT; OPERATE; CARD; READ; INTERFACE; CIRCUIT; EXCHANGE; CARD; INFORMATION; MEMORY; HOST; COMPUTER; IC; CARD; OWNER; FINGERPRINT
Derwent Class: S05; T01; T04; T05
International Patent Class (Main): G06K-019/10
International Patent Class (Additional): G06F-019/00; G06K-017/00; G06K-019/07
File Segment: EPI

DIALOG(R)File 347:JAPIO

06778470 **Image available**

IC CARD IDENTIFIED BY FINGERPRINT

PUB. NO.: **2001-005945** [JP 2001005945 A]
PUBLISHED: January 12, 2001 (20010112)
INVENTOR(s): CHIN MEISHO
APPLICANT(s): CHIN MEISHO
APPL. NO.: 11-229629 [JP 99229629]
FILED: August 16, 1999 (19990816)
PRIORITY: 88209054 [TW 88209054], TW (Taiwan), June 03, 1999 (19990603)
INTL CLASS: G06K-019/10; G06F-019/00; G06K-017/00; G06K-019/07

ABSTRACT

PROBLEM TO BE SOLVED: To obtain an IC card which reduces danger due to a card loss and leaving the IC card behind, improve the safety and convenience on Internet transactions and is identified by fingerprint.

SOLUTION: This IC card 1 which is accessed by a card reader 2 forming a communication link with a host computer 3, is respectively provided with a card body 18, and a memory device 11, a fingerprint sensor 12, a card reader interface circuit 13 and a microprocessor 14 that compares fingerprint scanned data received from the sensor 12 with fingerprint collation data in the device 11, operates the circuit 13 to exchange card information with the computer 3 through the reader 2 when the microprocessor 14 confirms that the holder of the body 18 is a legal user, which are respectively provided on the body 18.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－5945
（P2001－5945A）
(43)公開日　平成13年１月12日(2001.1.12)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｋ　19/10		Ｇ０６Ｋ　19/00	Ｓ	５Ｂ０３５
Ｇ０６Ｆ　19/00		17/00	Ｖ	５Ｂ０５５
Ｇ０６Ｋ　17/00		Ｇ０６Ｆ　15/30	３３０	５Ｂ０５８
19/07			３５０Ｚ	
		Ｇ０６Ｋ　19/00	Ｊ	

審査請求 有　請求項の数18　ＯＬ　（全７頁）

(21)出願番号　特願平11－229629
(22)出願日　平成11年８月16日(1999.8.16)
(31)優先権主張番号　８８２０９０５４
(32)優先日　平成11年６月３日(1999.6.3)
(33)優先権主張国　台湾（ＴＷ）

(71)出願人　599114885
沈　明　祥
台湾雲林縣斗南鎮新崙路15号
(72)発明者　沈　明　祥
台湾雲林縣斗南鎮新崙路15号
(74)代理人　100060069
弁理士　奥山　尚男　（外３名）

Ｆターム(参考)　5B035 AA14 BB09 BC01
5B055 EE02 EE03 HB02 JJ02 JJ05
KK05
5B058 KA38

(54)【発明の名称】　指紋によって識別されるＩＣカード

(57)【要約】
【課題】　カード紛失や置忘れによる危険性を低めて、インターネット取引上における安全性及び便利性を向上させるようにした、指紋によって識別されるＩＣカードを提供する。
【解決手段】　ホストコンピュータ３と通信リンクを形成するカードリーダー２によりアクセスされるＩＣカード１であって、札体１８と、この札体１８にそれぞれ設けられるメモリー装置１１，指紋センサ１２，及びカードリーダーインターフェース回路１３と、指紋センサ１２から受取った指紋走査データをメモリー装置１１で指紋照合データと比較して、札体１８の所有者が正当使用者であると確認すれば、カードリーダーインターフェース回路１３を作動してカードリーダー２を介してホストコンピュータ３とカード情報を交換するマイクロプロセッサー１４とをそれぞれ備える。

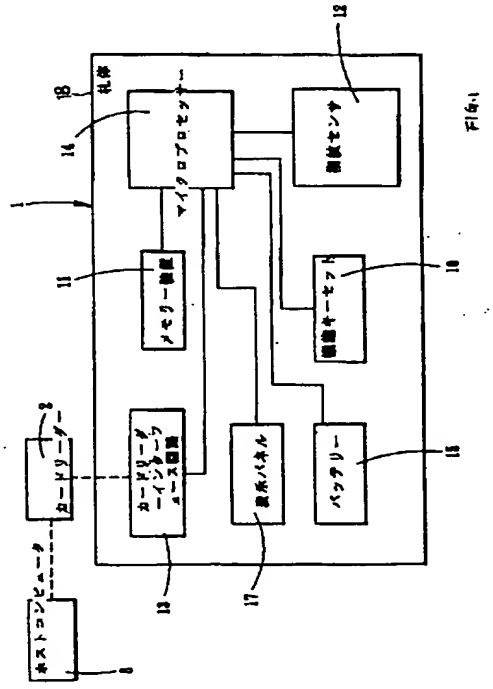

Fig.1

【特許請求の範囲】

【請求項１】　ホストコンピュータと通信リンクを形成するカードリーダーによりアクセスされるＩＣカードであって、

札体と、

上記札体に設けられて、正当使用者の指紋を走査して得られた指紋照合データ、及びカード情報を記憶するメモリー装置と、

上記札体に設けられて、上記札体所有者の指紋を走査して指紋走査データを生成する指紋センサと、

上記札体に設けられて、カードリーダーと通信するように作動できるカードリーダーインターフェース回路と、

上記札体に設けられて、上記メモリー装置、指紋センサ、及びカードリーダーインターフェース回路に接続され、上記指紋センサから受取った指紋走査データを上記メモリー装置で上記指紋照合データと比較して、上記札体の所有者が正当使用者であると確認した場合は、上記カードリーダーインターフェース回路を作動してカードリーダーを介してホストコンピュータとカード情報の交換をするマイクロプロセッサーと、をそれぞれ具備することを特徴とする指紋によって識別されるＩＣカード。

【請求項２】　上記指紋センサが指紋走査区域を区画したｍ×ｎ行列の走査セルを含むことを特徴とする請求項１に記載の指紋によって識別されるＩＣカード。

【請求項３】　上記指紋走査データが上記走査セル配列の対応ラインを走査して得られた多数の走査線を含むことを特徴とする請求項２に記載の指紋によって識別されるＩＣカード。

【請求項４】　上記走査セル配列の走査線が上記走査セル配列の行方向であることを特徴とする請求項３に記載の指紋によって識別されるＩＣカード。

【請求項５】　上記走査セル配列の走査線が上記走査セル配列の列方向であることを特徴とする請求項３に記載の指紋によって識別されるＩＣカード。

【請求項６】　上記各走査セルが、札体所有者の指紋の隆起紋を検出した場合は第１のロジックシグナルを発生して、札体所有者の指紋の谷底紋を検出した場合は第２のロジックシグナルを発生することを特徴とする請求項２に記載の指紋によって識別されるＩＣカード。

【請求項７】　上記指紋照合データが多数の走査線データを含み、各走査線データが正当使用者の指紋のそれぞれ走査線指紋の特徴を記述してあることを特徴とする請求項１に記載の指紋によって識別されるＩＣカード。

【請求項８】　上記札体に設けられて上記マイクロプロセッサーに接続された機能キーセットを備え、上記機能キーセットが上記ホストコンピュータとの交換カード情報を選択するようにしたことを特徴とする請求項１に記載の指紋によって識別されるＩＣカード。

【請求項９】　上記札体に設けられて上記マイクロプロセッサーに接続されて制御される表示パネルを備え、上記ホストコンピュータと交換するカード情報を表示させるようにしたことを特徴とする請求項１に記載の指紋によって識別されるＩＣカード。

【請求項１０】　上記マイクロプロセッサーが、上記札体所有者が正当使用者であると確認した状態の下で、上記メモリー装置が記憶している指紋照合データのセグメントを上記ホストコンピュータに伝送するようにしたことを特徴とする請求項１に記載の指紋によって識別されるＩＣカード。

【請求項１１】　上記マイクロプロセッサーが、上記札体所有者が正当使用者であると確認した下で、上記メモリー装置が記憶している指紋照合データのセグメントをホストコンピュータに伝送するようにしたことを特徴とする請求項７に記載の指紋によって識別されるＩＣカード。

【請求項１２】　上記指紋照合データのセグメントが、上記ホストコンピュータと交換するカード情報の期日に対応して選択した走査線データの何れか一つを含むことを特徴とする請求項１１に記載の指紋によって識別されるＩＣカード。

【請求項１３】　上記指紋照合データのセグメントが、上記ホストコンピュータと交換するカード情報の時間に対応して選択した走査線データの何れか一つを含むことを特徴とする請求項１１に記載の指紋によって識別されるＩＣカード。

【請求項１４】　上記指紋照合データのセグメントが、ランダムに選択した走査線データの何れか一つを含むことを特徴とする請求項１１に記載の指紋によって識別されるＩＣカード。

【請求項１５】　上記ホストコンピュータと交換するカード情報がクレジットカードナンバーを含むことを特徴とする請求項１に記載の指紋によって識別されるＩＣカード。

【請求項１６】　上記ホストコンピュータと交換するカード情報が銀行取引口座ナンバーを含むことを特徴とする請求項１に記載の指紋によって識別されるＩＣカード。

【請求項１７】　上記ホストコンピュータと交換するカード情報が正当使用者の身分証明カードナンバーを含むことを特徴とする請求項１に記載の指紋によって識別されるＩＣカード。

【請求項１８】　上記メモリー装置がフラッシュメモリーであることを特徴とする請求項１に記載の指紋によって識別されるＩＣカード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＩＣカードに関し、特に、指紋を所有者と使用者の同定に利用するＩＣカードに関する。

【０００２】

【従来の技術】因みに、金融活動や科学技術の進歩に伴い、近年では、消費する際に大量の現金を持ち合せなくても、プラスチック通貨、例えばクレジットカード、キャッシュカード等を利用して購買を行える。この種のプラスチック通貨の便利性から、人々の携帯しているプラスチック通貨は、往々にして一枚だけに止まらず、且つその他のカード、例えば身分証明カードや出入証明カード等をも携帯するので、これらのカードが紛失でもすると、所有者は他人が冒認使用する危険に晒されることとなる。従って、このような危険の確率を最低限に抑えることができれば、所有者の損害を軽くすることができる。そこで、例えば人間のそれぞれの指紋が異なることを利用して、これらのカードの所有者を識別できるようにすれば、カードが他人に悪用される可能性を最低限に低められる筈である。また、インターネットにより伝送した際に、しばしばデータがインターセプトされることがあって、近年流行っているインターネット上での取引において、カード関連データの伝送過程における安全性がますます重要視され、若しもインターネットでインターセプトされたデータが他人に使用され得ないのであれば、所有者にとって権益がより保障される筈である。なお、このように多数のカード、例えばクレジットカード、キャッシュカード、身分証明等を携帯して、もしもそのうちの何れかを使用する際は、往々にして多数のカード中から捜し出さなければならないので、不便で煩わしいばかりでなく、多数のカードが嵩張ってスペースを占めることとなるが、もしも一枚のカードでこれらカードに取って代れるものならば、生活上の便利性が一層向上する筈である。

【０００３】

【発明が解決しようとする課題】本発明は、上記問題点に鑑みてなされたものであって、その目的は、カード紛失や置忘れによる危険性を低めて、インターネット取引上における安全性及び便利性を向上させるようした、指紋によって識別されるＩＣカードを提供することにある。

【０００４】

【課題を解決するための手段】上記目的を達成するため、本発明に係る指紋によって識別されるＩＣカードは、ホストコンピュータとで通信リンクを形成するカードリーダーによってアクセスされ、上記ＩＣカードが札体、上記札体に設けられるメモリー装置、上記札体に設けられる指紋センサ、上記札体に設けられるカードリーダーインターフェース回路、及び上記札体に設けられて上記メモリー装置、指紋センサ及びカードリーダーインターフェース回路に接続されるマイクロプロセッサーを含んでおり、上記メモリー装置が正当使用者の指紋を走査して得られた指紋照合データ及びカード情報を記憶し、上記指紋センサが札体所有者の指紋を走査して指紋走査データを生成し、上記カードリーダーインターフェース回路が作動してカードリーダーと通信できて、上記マイクロプロセッサーが指紋センサから指紋走査データを受けると、上記指紋走査データとメモリー装置にある指紋照合データとを比較して、両方が一致すれば正当使用者が札体所有者であると判定し、上記カードリーダーインターフェース回路を作動してカードリーダーを介してホストコンピュータとカード情報を取引するように構成される。

【０００５】上記のように構成された本発明のＩＣカードは、ＩＣカード所有者の指紋を走査して得られた指紋走査データとメモリー装置に記憶された正当使用者の指紋照合データを比較して、正当使用者が所有者であると確認されてから使用できる。また、ＩＣカードが時間や期日の関連条件を選択してなる指紋照合データのセグメントを伝送できるので、ホストコンピュータとの取引カード情報を機動的に変化させることができる。さらに、ＩＣカード一枚でバンクカード、身分証明カード或いはクレジットカードとして使用できるので、単に一枚のカードだけを携帯して色々な役目を果すことができる。

【０００６】

【発明の実施の形態】以下、本発明を実施の形態に基づいて具体的に説明するが、本発明はこの例だけに限定されない。

【０００７】図１は、本発明における比較的好ましい実施形態のブロック図で、図示の如く、本実施形態の指紋によって識別されるＩＣカード１は、ホストコンピュータ３とで通信リンクを形成するカードリーダー（Card Reader）２によってアクセスされる。このカードリーダー２は、ほとんどがパブリックゾーン、例えば商店、デパートメント等に取付けられ、上記ホストコンピュータ３は、銀行、クレジットカードセンター等に設けられる。ＩＣカード１は、札体１８、及びこの札体１８にそれぞれ取付けられるメモリー装置１１、指紋センサ１２、カードリーダーインターフェース回路１３、マイクロプロセッサー１４、バッテリー１５、機能キーセット１６及び表示パネル１７を含んでいる。

【０００８】上述のメモリー装置１１は、フラッシュメモリー（FLASH MEMORY）であって、正当使用者またはカード体所有者の指紋を走査して得られた指紋照合データ及び正当使用者のデータ情報、例えば身分証明証ナンバー、銀行口座ナンバー、クレジットカードナンバー等を記憶してあり、この指紋照合データは多数のそれぞれが正当使用者の指紋における各走査線の指紋の特徴を記述した走査線データを含んでいる。

【０００９】上述の指紋センサ１２は、正当使用者の指紋５（図２参照）を走査するものであり、正当使用者またはカード所有者の指紋５に対応する指紋走査データを生成する。図２に示す如く、この指紋センサ１２は、ｍ×ｎ行列の走査セルを含んだ指紋走査区域Ｍを備えており、この指紋走査データは、多数の走査セルの行列ライ

ンを走査して得られた走査線データを含む。走査セルの行列ラインは、列方向或いは行方向の走査ができて、例えば、m＝３０、n＝４５の場合、列方向の第１の走査線Ｉが（1、n；n＝1～４５）で、列方向の第２の走査線ＩＩが（2、n；n＝1～４５）で、列方向の最後の走査線ＩＩＩ、すなわち第３０の走査線ＩＩＩが（３０、n；n＝1～４５）である。また、行方向の第１の走査線ＩＶが（m、1；m＝1～３０）で、行方向の第２の走査線Ｖが（m、2；m＝1～３０）で、行方向の最後の走査線ＶＩ、即ち第４５の走査線ＶＩが（m、４５；m＝1～３０）である。そして、札体１８の所有者の指紋の隆起紋が検出されると、走査セルがハイ・ロジックシグナルを発生し、札体１８の所有者の指紋の谷底紋が検出されると、走査セルがロー・ロジックシグナルを発生する。

【００１０】図３は、指紋センサ１２が列方向の第１の走査線Ｉを走査した際に、走査セル（1，１３）、（1，１５）がそれぞれハイ・ロジックシグナルを生じて、他の走査セルがロー・ロジックシグナルを発生したことを示している。図４は、列方向の第２の走査線ＩＩを走査して得られた走査線データを示している。図５は、行方向の第１の走査線ＩＶを走査して得られた走査線データを示している。すなわち、指紋のユニークな特徴を考えると、もしもカード所有者が正当使用者と異なれば指紋走査データも指紋照合データと異なる。

【００１１】上述のカードリーダーインターフェース回路１３は、作動されてカードリーダー２と通信することができる。

【００１２】上述のマイクロプロセッサー１４は、指紋センサ１２、メモリー装置１１及びカードリーダーインターフエース回路１３と接続されていて、上記指紋センサ１２から指紋走査データを受け、そしてメモリー装置１１において指紋走査データと指紋照合データとを比較して、正当使用者が札体１８の所有者であると同定すれば、マイクロプロセッサー１４がカードリーダーインターフェース回路１３を作動して、正当使用者がカード所有者であると確認した状態の下でカードリーダー２を介してホストコンピュータ３とカード情報とを交換する。従って、正当使用者がカード所有者ででないと、ＩＣカードを使用することができない。

【００１３】上述のバッテリー１５は、マイクロプロセッサー１４に接続されて、ＩＣカード１に必要な電源を供給する。

【００１４】上述の機能キーセット１６は、マイクロプロセッサー１４に接続されており、ホストコンピュータ３と取引されるカード情報を選択して操作することができる。例えば、機能キーセット１６がクレジットカードモードに選択されると、ホストコンピュータ３と取引するカード情報は、クレジットカードナンバーを含んでいる。そして、ネットワーク取引の安全性を高めるため、正当使用者が札体１８の所有者であると確認した状態の下で、マイクロプロセッサー１４によってホストコンピュータ３に転送される指紋照合データのセグメントをメモリー装置１１に記憶するのがより好ましい。指紋照合データのセグメントは、ホストコンピュータ３と交換したカード情報の期日或いは時間に応じて、選択した走査線データの何れかを選ぶことができ、または走査線データの一つをランダムに選択することもできる。

【００１５】ここで、一例を挙げると、指紋照合データの各走査線データに番号を付けて、指紋走査区域Ｍの列方向の偶数走査ラインの走査データを数"０"に設定して、指紋走査区域Ｍの列方向の奇数走査ラインの走査データを数"１"に設定し、指紋走査区域Ｍの行方向の偶数走査ラインの走査データを数"２"に設定して、指紋走査区域Ｍの行方向の奇数走査ラインの走査データを数"３"に設定する。そして、選択条件が時間２：３０であると、カードリーダー２のアクセスから指紋照合データのセグメントが数２，３，０の走査線データと対応して、０－２－３－０の順序でホストコンピュータ３に転送され、このホストコンピュータ３が指紋照合データのセグメントと選択時間条件でホストコンピュータ３に記憶された指紋照合データを比較する。他方の例では、選択条件が４：３３　５／３／１９９９の時間と期日であると、カードリーダー２のアクセスにより指紋照合データのセグメントが数０，１，３，４，９，５の走査線データと対応して、１－９－９－９－０－５－０－３－０－４－３－３の順序でホストコンピュータ３に転送される。すなわち、指紋照合データのセグメントの機動的交換により特定条件、例えば４：３３　５／３／１９９９の下で妥当なＩＣカードの使用取引行為を安全にする。換言すると、特定時間及び期日で生じるＩＣカード１の転送カード情報が許可なきコピーであるとき、或いはカード情報が他の時間や期日で使用する不当な取引は、結果として、ホストコンピュータ３に拒絶される。

【００１６】上述の表示パネル１７は、マイクロプロセッサー１４とに接続されており、ホストコンピュータ３との交換カード情報を表示するように制御される。この表示パネル１７は、ホストコンピュータ３からの、例えば合計金額や収支バランス等をも表示する。

【００１７】以上を要約すると、本実施形態の指紋によって識別されるＩＣカードは、ホストコンピュータ３と通信リンクを形成するカードリーダー２によりアクセスされるＩＣカード１であって、札体１８と、札体１８に設けられて、正当使用者の指紋を走査して得られた指紋照合データ、及びカード情報を記憶するメモリー装置１１と、札体１８に設けられて、札体１８所有者の指紋を走査して指紋走査データを生ずる指紋センサ１２と、札体１８に設けられて、カードリーダー２と通信するように作動できるカードリーダーインターフェース回路１３と、札体１８に設けられて、メモリー装置１１、指紋セ

ンサ１２及びカードリーダーインターフェース回路１３と連結し、指紋センサ１２から受取った指紋走査データをメモリー装置１１で指紋照合データと比較して、札体１８の所有者が正当使用者であると確認すれば、カードリーダーインターフェース回路１３を作動してカードリーダー２を介してホストコンピュータ３とカード情報を交換するマイクロプロセッサー１４とをそれぞれ備えて成るものである。

【００１８】

【発明の効果】上記のように構成された本発明によれば、下記のような優れた作用効果を奏することができる。

（１）　ＩＣカード１がＩＣカード所有者の指紋を走査して得られた指紋走査データとメモリー装置１１の指紋照合データとを比較して、正当使用者が所有者であると確認されると、上記ＩＣカード１は正当使用者だけに使用されるので、ＩＣカード１が紛失或いは置忘れた際に伴う危険性を低減することができる。

（２）　ＩＣカード１が時間や期日の関連条件を選択してなる指紋照合データのセグメントを伝送できるので、ホストコンピュータ３との交換カード情報を機動的に変化させることができ、従って、インターネット取引の際の安全性を向上させることができる。

（３）　ＩＣカード１をバンクカード、身分証明カード或いはクレジットカードとして使用できるので、使用者は単に１枚のカードだけを携帯して色々な異なる役割を果すことができ、より便利になる。

【図面の簡単な説明】

【図１】本発明の比較的好ましい実施形態に係るＩＣカードの構成を示す電気回路ブロック図である。

【図２】本発明の実施形態における指紋センサの指紋走査区域を示す図である。

【図３】図２で示した列方向の第１の走査線Ｉの走査線データを表示する図である。

【図４】図２で示した列方向の第２の走査線Ｉの走査線データを表示する図である。

【図５】図２で示した行方向の第１の走査線Ｉの走査線データを表示する図である。

【符号の説明】

１　ＩＣカード
２　カードリーダー
３　ホストコンピュータ
５　指紋
１１　メモリー装置
１２　指紋センサ
１３　カードリーダーインターフェース回路
１４　マイクロプロセッサー
１５　バッテリー
１６　機能キーセット
１７　表示パネル

【図１】

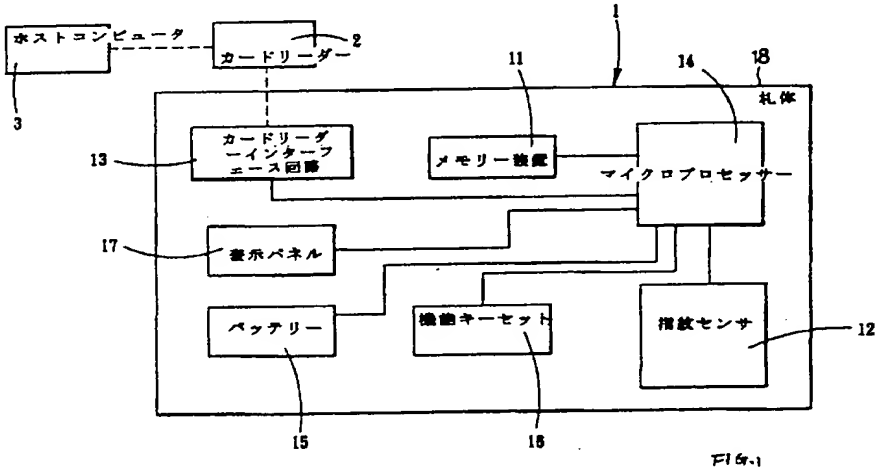

Fig.1

【図２】

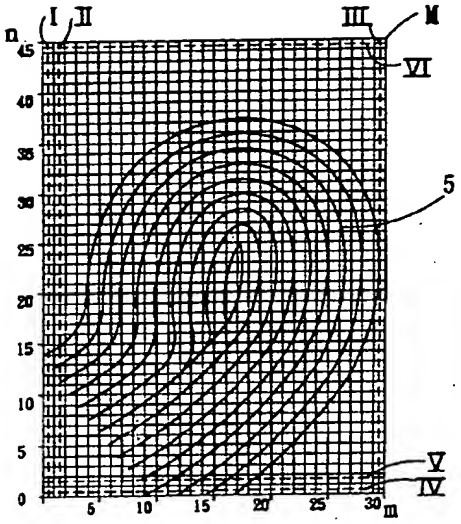

FIG.2

【図５】

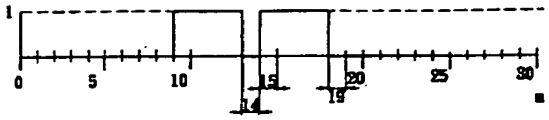

FIG.5

【図３】

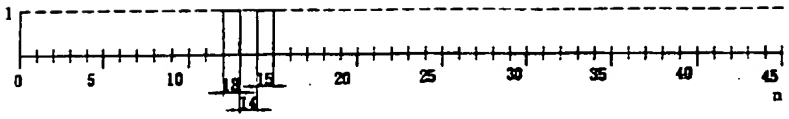

FIG.3

【図４】

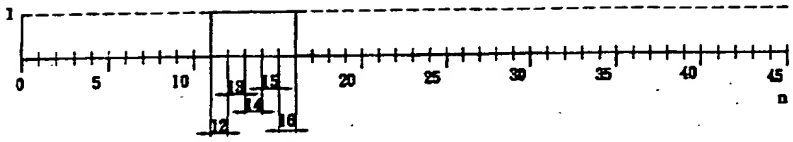

FIG.4